Chapter 8

Cryptography
Standards

Cryptography Standards and Protocols

- **NSA:** The *National Security Agency (NSA)* is responsible for creating codes, breaking codes, and coding systems for the U.S. government.
  - This agency was chartered in 1952. It tries to keep a low profile; for many years, the government didn’t publicly acknowledge its existence.
- **NSA/CSS:** The National Security Agency/Central Security Service (NSA/CSS) is an independently functioning part of the NSA.
  - It was created in the early 1970s to help standardize and support Department of Defense (DoD) activities.
  - The NSA/CSS supports all branches of the military.

Cryptography Standards and Protocols

- **NIST:** The*National Institute of Standards and Technology*, known as the National Bureau of Standards (NBS) .
  - NIST has become very involved in cryptography standards, systems, and technology in a variety of areas.
- **ABA:** The American Bankers Association has been very involved in the security issues facing the banking and financial industries.
  - Banks need to communicate with each other in a secure manner.
  - The ABA sponsors and supports several key initiatives regarding financial transactions.

Cryptography Standards and Protocols

- **IETF:** The *Internet Engineering Task Force (IETF)* is an international community of computer professionals
  - network engineers, vendors, administrators, and researchers.
  - The IETF is mainly interested in improving the Internet; it’s also very interested in computer security issues.
  - The IETF uses working groups to develop and propose standards.
- **ISOC:** The *Internet Society (ISOC)* is a professional group whose membership consists primarily of Internet experts.
  - The ISOC oversees a number of committees and groups, including the IETF.

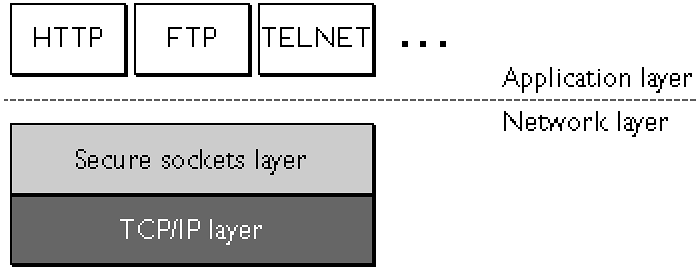
Cryptography Standards and Protocols

- **W3C:** The *World Wide Web Consortium (W3C)* is an association concerned with the interoperability, growth, and standardization of the World Wide Web
  - the primary sponsor of XML and other web-enabled technologies.
- **ITU:** The *International Telecommunications Union* is responsible for virtually all aspects of telecommunications and radio communications standards worldwide.
- **CCITT:** The Comité Consultatif International Téléphonique et Télégraphique: committee has been involved in developing telecommunications and data communications standards.
- **IEEE:** The *Institute of Electrical and Electronics Engineers:* is an international organization focused on technology and related standards.

Protocols: Secure Sockets Layer (SSL)

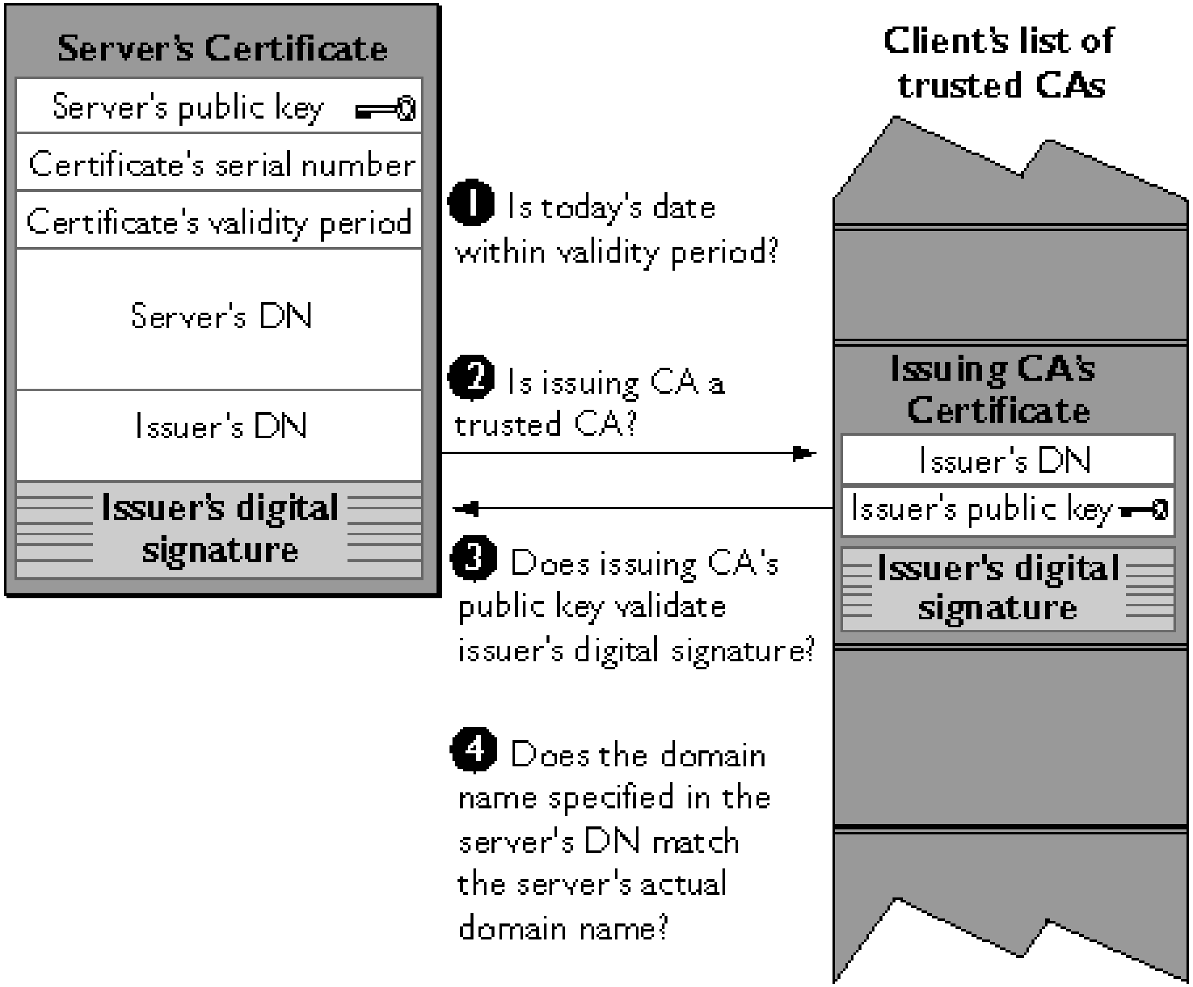
- Developed by Netscape
- Uses public key encryption to secure channel over public Internet
- *SSL* is used to establish a secure communication connection betweentwo TCP-based machines.
- Provides privacy
    - Encrypted connection
        - Confidentiality and tamper-detection
- Provides authentication
    - Authenticate server
    - Authenticate client optionally

Protocols: Secure Sockets Layer (SSL)

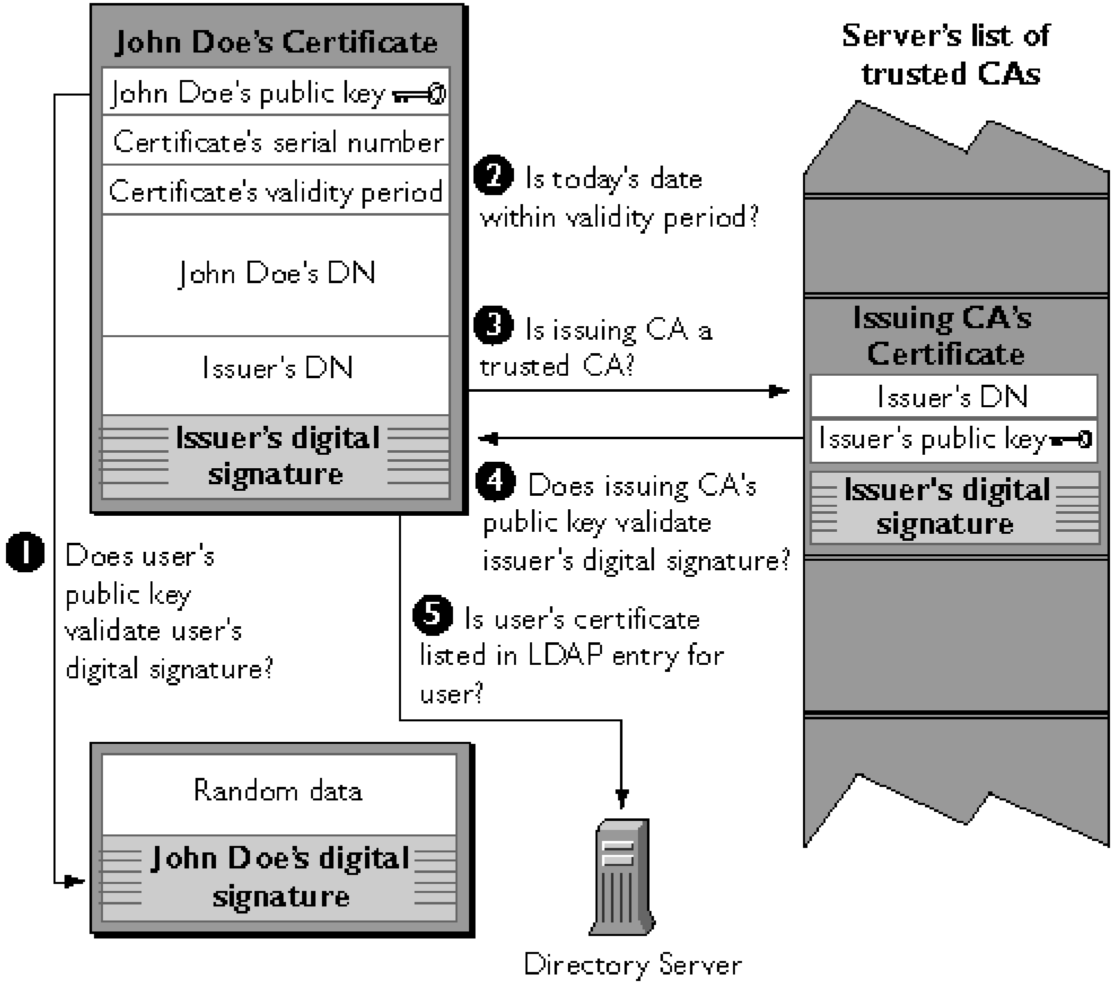


- Lies above transport layer, below application layer
  - Can lie atop any transport protocol, not just TCP/IP
  - Runs under application protocols like HTTP, FTP, and TELNET

SSL: Server Authentication


Server's Certificate
Server's public key
Certificate's serial number
Certificate's validity period
Server's DN
Issuer's DN
Issuer's digital signature
Client's list of trusted CAs
❶ Is today's date within validity period?
❷ Is issuing CA a trusted CA?
Issuing CA's Certificate
Issuer's DN
Issuer's public key
Issuer's digital signature
❸ Does issuing CA's public key validate issuer's digital signature?
❹ Does the domain name specified in the server's DN match the server's actual domain name?

SSL: Client Authentication

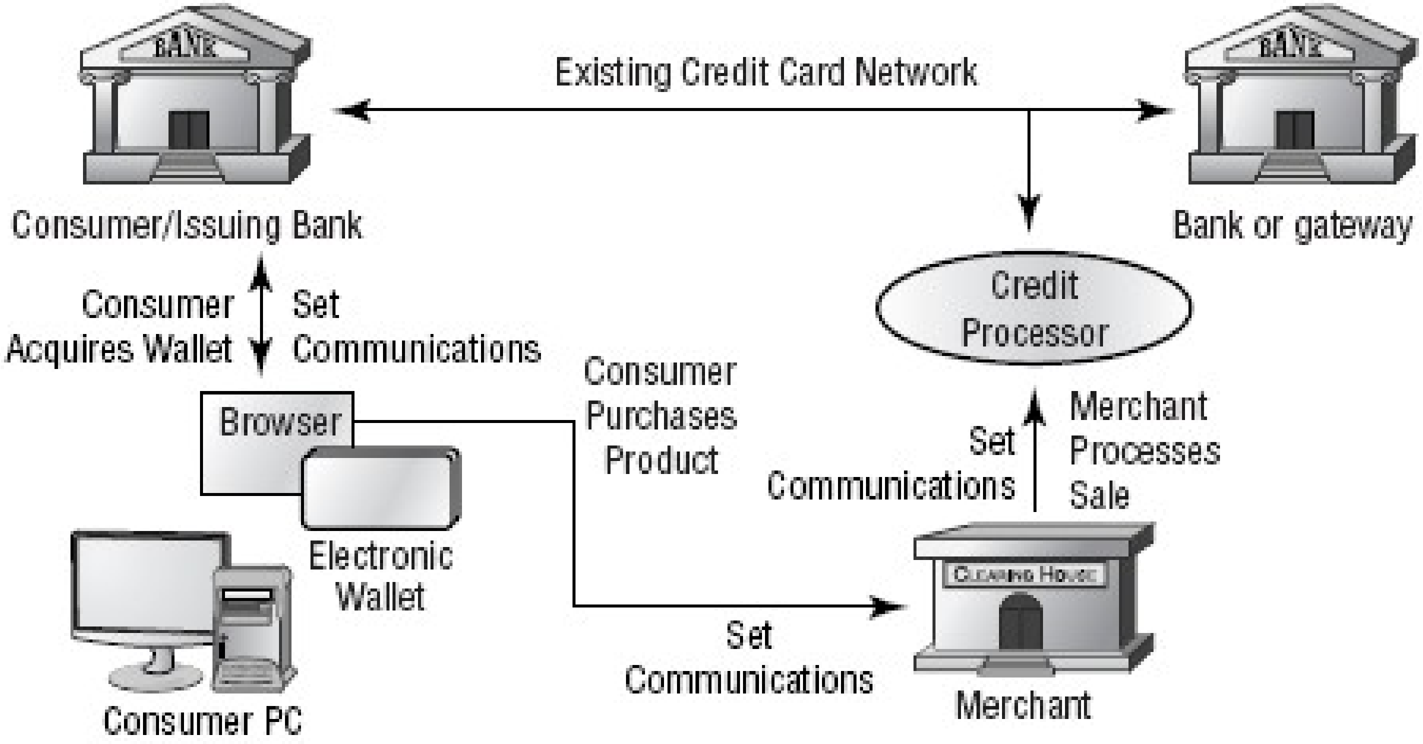

John Doe's Certificate
John Doe's public key
Certificate's serial number
Certificate's validity period
John Doe's DN
Issuer's DN
Issuer's digital signature
Server's list of trusted CAs
2 Is today's date within validity period?
3 Is issuing CA a trusted CA?
Issuing CA's Certificate
Issuer's DN
Issuer's public key
Issuer's digital signature
4 Does issuing CA's public key validate issuer's digital signature?
1 Does user's public key validate user's digital signature?
5 Is user's certificate listed in LDAP entry for user?
Random data
John Doe's digital signature
Directory Server

Protocols: *Secure Electronic Transaction (SET)*

- *SET* provides encryption for credit card numbers that can betransmitted over the Internet.
- It was developed by Visa and MasterCard
- Works in conjunction with an electronic wallet that must be set up in advance of the transaction
- An *electronic wallet* is a device that identifies you electronically in the same way as the cards you carry in your wallet.

Protocols: *Secure Electronic Transaction (SET)*

FIGURE 8.3 The SET transaction in process



Protocols: S-HTTP

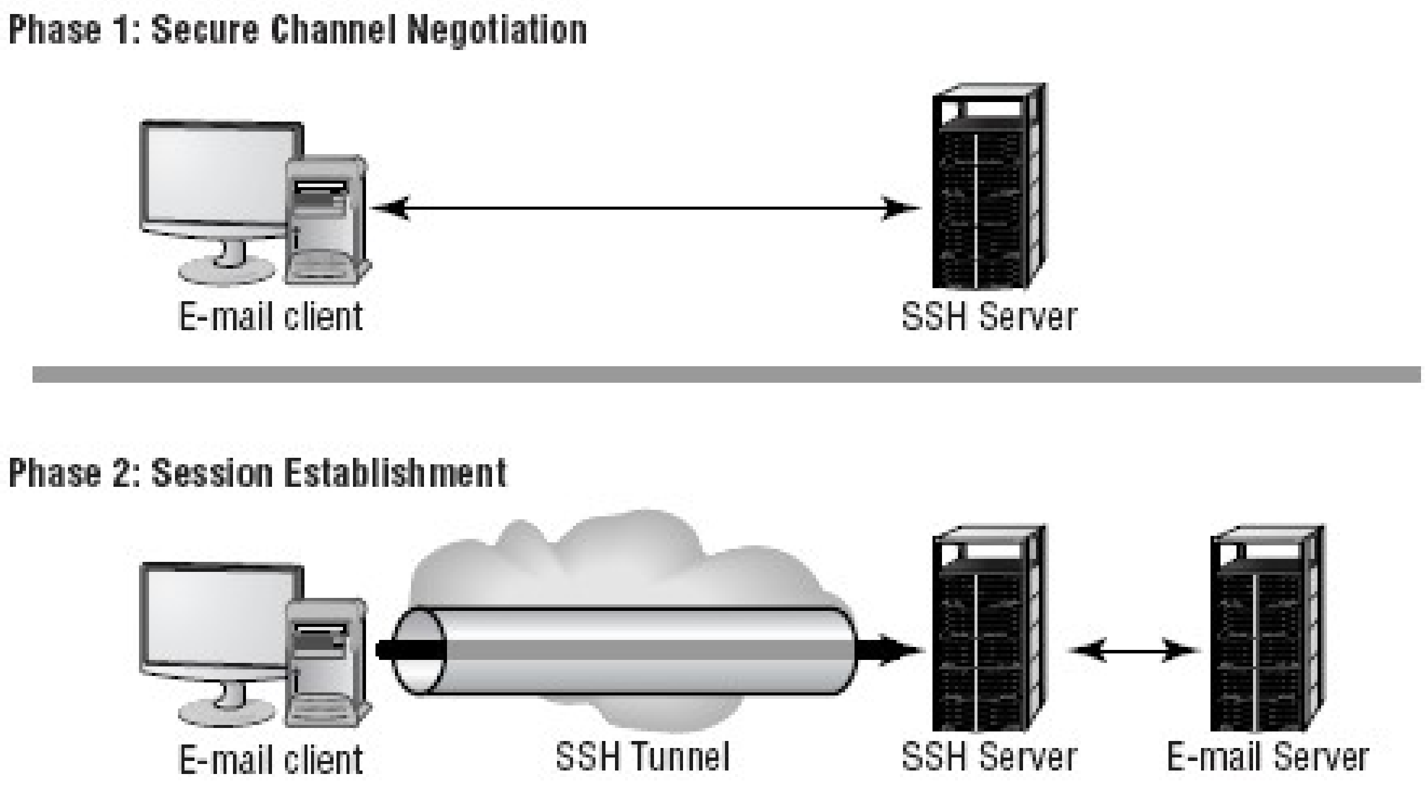
- Secure Hypertext Transfer Protocol (S-HTTP): extended version of Hypertext Transfer Protocol; provides for encryption of individual messages between client and server across Internet
- S-HTTP is the application of SSL over HTTP; allows encryption of information passing between computers through protected and secure virtual connection

Protocols: *Secure Shell (SSH)*

- *Secure Shell (SSH)* is a tunneling protocol originally used on Unix systems.
- The handshake process between the client and server is similar to the process described in SSL.
- SSH is primarily intended for interactive terminal sessions.
- SSH connections are established in two phases:
  - The first phase is a secure channel to negotiate the channel connection
  - The second phase is a secure channel used to establish the connection.

Protocols: *Secure Shell (SSH)*

FIGURE 8.4 The SSH connection-establishment process

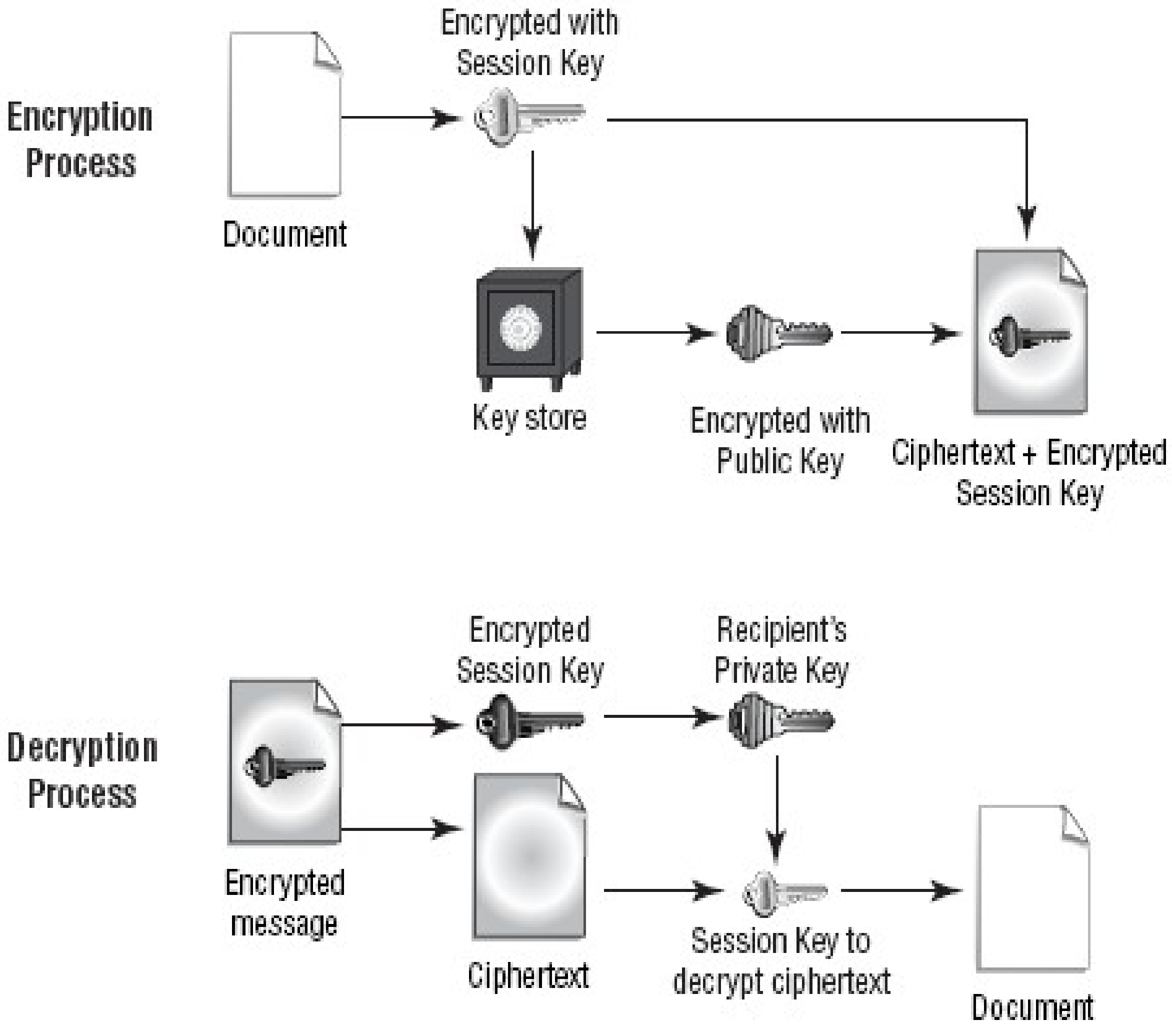


Pretty Good Privacy (PGP)

- Pretty Good Privacy (PGP) is a freeware e-mail encryption system.
- PGP was introduced in the early 1990s, and it’s considered to be a very good system
- PGP uses both symmetrical and asymmetrical systems
- During the encryption process, the document is encrypted with the public key and also a session key, which is a one-use random number, to create the ciphertext.

Pretty Good Privacy (PGP)

FIGURE 8.5 The PGP encryption system



Key Management and the Key Life Cycle

- ~~*Key management* refers to the process of working~~ with keys from the time they are created until the time they are retired or destroyed.
- Key management includes
  - Centralized versus decentralized key generation
  - Key storage and distribution
  - Key escrow
  - Key expiration
  - Key revocation
  - Key suspension
  - Key recovery and archival
  - Key renewal
  - Key destruction
  - Key usage

Comparing Centralized and Decentralized Key Generation

- *Key generation* is an important first step in the process of working withkeys and certificates.
- Centralized generation allows the key-generating process to take advantage of large-scale system resources.
- By usinga centralized server, this process can be managed with a large single system.
- Centralized generation has the advantage of allowing additional management functions tobe centralized.
- A major disadvantage is that the key archival and storage process may be vulnerable to an attack against a single point instead of a network.

Comparing Centralized and Decentralized Key Generation

- Decentralized key generation allows the key-generating process to be pushed out into the organization or environment.
- The advantage of this method is that it allows work to be decentralized and any risks to be spread.
- This system isn’t vulnerable to a single-point failure or attack.

Comparing Centralized and Decentralized Key Generation

FIGURE 8.6 A centralized key-generating facility

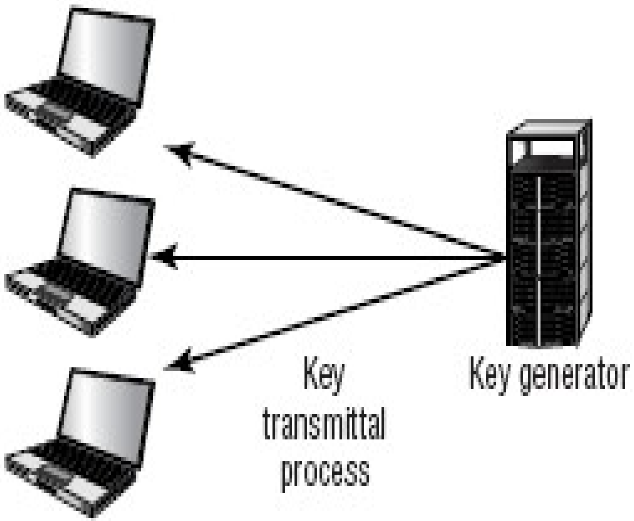
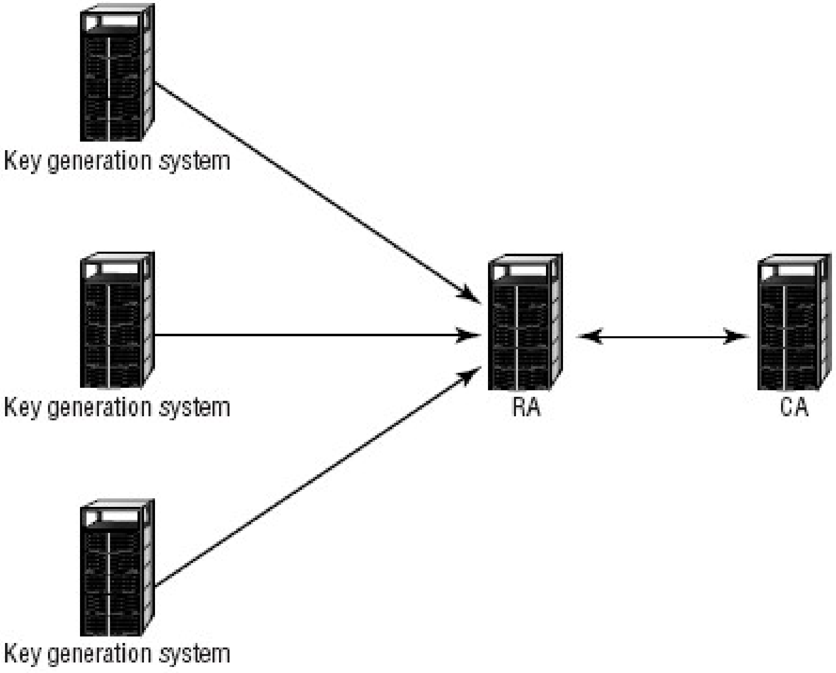


FIGURE 8.7 A distributed key-generating system



Storing and Distributing Keys

- Distributing keys is usually accomplished using:
  - *Key Distribution Center (KDC)*,
  - *Key Exchange Algorithm (KEA)*,
- A KDC is a single service or server that stores, distributes, and maintains cryptographic session keys.
- The KEA negotiates a secret key between the two parties; the secret key is a short-term, single-use key intended strictly for key distribution.

Storing and Distributing Keys

FIGURE 8.8 The KDC process in a Kerberos environment

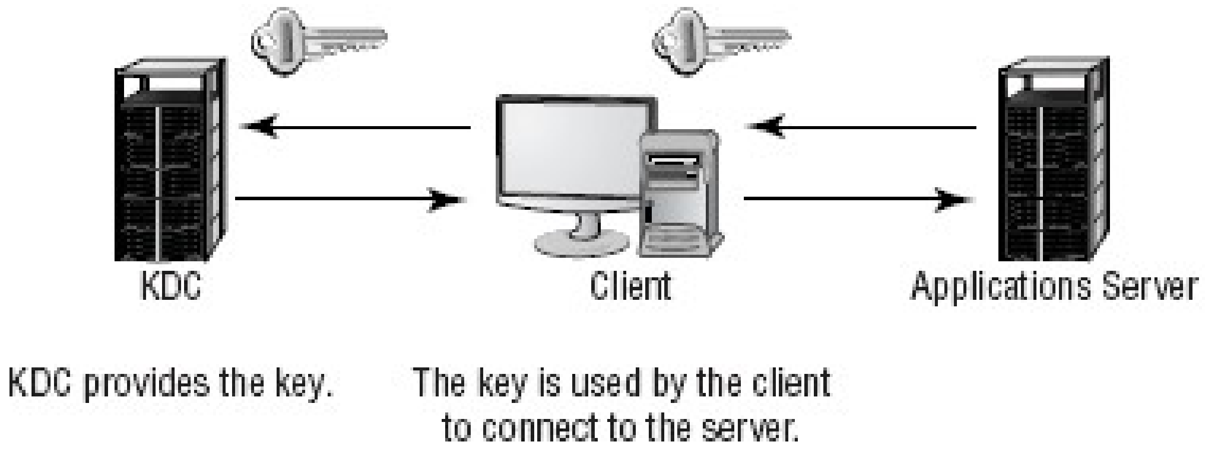
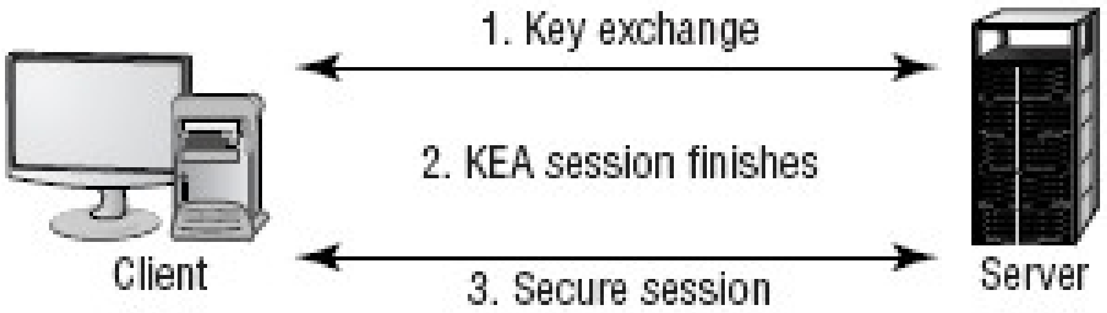


FIGURE 8.9 The KEA process



Key Management

- A *key escrow* system stores keys for the purpose of law enforcement access.
  - *Key escrow* refers to both a process and an organization or system that stores keys for access at a later date.
- A key expiration date identifies when a key is no longer valid.
  - Keys with expiration dates work similarly to credit cards that expire.
  - Most applications that are key-enabled or certificate-enabled check the expiration date on a key and report to the user if the key has expired.
- Keys are revoked when they are compromised, the authentication process has malfunctioned, people are transferred, or other security risks occur.

Recovering and Archiving Keys

- Archiving old keys is essential: Any time a user or key generator creates and issues a key, the key must also be sent to the key archive system.
- Key recovery is an important part of an encryption system.
- Information that is stored using older keys will be inaccessible using a new key.
  - **Current Keys** are the keys in use at the present time.
  - **Previous Keys** have recently expired and are no longer current.
  - **Archived Keys** were discussed earlier.

Key Management

- **Renewing Keys:** A key would be reissued for a certain time: This process is called a *key rollover*.
- Many systems provide a way to renew existing keys, rather than rolling them over.

- **Destroying Keys:** is the process of destroying keys that have become invalid.
    - For example, an electronic key can be erased from a smart card.